Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)
NAI1P489/03.047.01

I hereby certify that this correspondence is being e-filed with the USPTO	Application Number	Filed
on January 31, 2008	10/755,450	01/13/2004
Signature /Dana Chan/	First Named Inventor: Igor Garrievich Muttik	
Typed or printed name Dana Chan	Art Unit: 2132	Examiner: Sandoval, Kristin D.

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

- ☐ applicant/inventor.
- ☐ assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)
- ☑ attorney or agent of record. Registration number 41,429
- ☐ attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____

/KEVINZILKA/
Signature

Kevin J. Zilka
Typed or printed name

408-971-2573
Telephone number

January 31, 2008
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☑ *Total of 1 forms are submitted.

REMARKS

In the Office Action mailed 05/22/2007, the Examiner rejected Claims 1-51 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Examiner specifically took issue with the following language from Claims 1, 7, 18, 24, 35 and 41 as being indefinite: "more strongly." In the Amendment filed 08/22/2007, applicant respectfully asserted that such claim language is to be read according to the plain and ordinary meaning thereof, in view of dictionary definitions, etc. The Examiner, however, argued that "it is uncertain what the association is stronger than." In response, applicant respectfully asserted that the association is stronger than it would be without the modification of the set of rules.

In the Office Action mailed 11/01/2007, has removed the rejection of Claims 1-51 under 35 U.S.C. 112, second paragraph, but has responded to applicant's above arguments. In particular, the Examiner has argued that applicant's above arguments are "not clear from the claim language," and that "it is not clear that the external program calls are more strongly associated with malicious computer program activity as compared to without the modifications." The Examiner has also argued that "[i]t could be more strongly associated with malicious computer program activity than the primary set of external program calls."

Applicant respectfully disagrees. For example, with respect to the independent claims, applicant clearly claims "modifying said set of rules **such that** said at least one secondary set of one or more external program calls are more strongly associated with malicious computer program activity" (see this or similar, but not necessarily identical language in the independent claims-emphasis added), as claimed.

The Examiner has rejected Claims 1, 2, 8-10, 13, 14, 17, 18, 19, 25-27, 30, 34, 35, 36, 42-44, 47, 48 and 51-53 under 35 U.S.C. 102(e) as being anticipated by van der Made (U.S. Patent No. 7,093,239). Applicant respectfully disagrees with such rejection.

With respect to independent Claims 1, 18 and 35, the Examiner has relied on Col. 6, lines 12-24; and Col. 11, lines 46-60 from the Made reference to make a prior art showing of applicant's claimed "secondary set identifying code operable to identify, within said stream, at least one secondary set of one or more external program calls associated with said primary set of one or more external program calls" (see this or similar, but not necessarily identical language in the independent claims).

Applicant respectfully points out that the Made reference excerpts relied upon by the Examiner merely teach "extracting a behavior pattern and sequence from a modified, new, unknown or suspect program," and that "[t]he behavior pattern is preferably used to analyze the behavior of the unknown program to determine if the behavior of the unknown program is malicious" (Col. 6, lines 13-17 – emphasis added). The excerpts from Made also teach that the "ABM engine then analyzes the first executable program and finds that its behavior pattern is altered in a manner indicating that a virus is active" (Col. 11, lines 57-59 – emphasis added).

However, applicant respectfully asserts that only generally disclosing that "[t]he behavior pattern is preferably used to analyze the behavior of the unknown program," as in Made, does not specifically meet a "secondary set of identifying code operable to identify, within said stream, at least one secondary set of one or more external program calls associated with said primary set of one or more external program calls" (emphasis added), particularly where the "primary set of one or more external program calls match[es] one or more rules indicative of malicious computer program activity from among a set of rules" (emphasis added), in the context claimed by applicant.

Furthermore, applicant respectfully points out that detecting active viruses based on whether an executable program's behavior pattern is altered, as in Made, clearly fails to teach the use of a "secondary set of identifying code operable to identify, within said stream, at least one secondary set of one or more external program calls associated with said primary set of one or more external program calls" (emphasis added), where the

"primary set of one or more external program calls match[es] one or more rules indicative of malicious computer program activity from among a set of rules" (emphasis added), in the context claimed by applicant. Simply nowhere in the excerpts relied on by the Examiner is there any teaching or suggestion of a "secondary set of one or more external program calls associated with said primary set of one or more external program calls," as claimed.

In the Office Action mailed 11/01/2007, the Examiner has referred to Col. 6, lines 43-63 in Made in arguing that "Made discloses pattern identifying code that can identify program calls associated with malicious activity and are also associated with another set of program calls such as ones that are content destructive since these calls are calls that are made as a result of the first set of calls detected by patterns."

Applicant respectfully disagrees. Col. 6, lines 43-63 in Made merely discloses that "the analysis procedure specifically targets infection methods such as, but not limited to, the insertion of code to other executables or documents, submitting code to other applications to be transmitted or stored, insertion of code into high memory blocks and the modification of memory control blocks," and that "the analysis method further look[s] for destructive content, such as, but not limited to, functions that overwrite disk areas or the BIOS ROM, or delete files or directories."

Clearly, Made merely teaches targeting particular infection methods, and separately looking for destructive content, which does not even suggest "identifying code that can identify program calls associated with malicious activity and are also associated with another set of program calls such as ones that are content destructive" (emphasis added), as the Examiner has noted. To this end, the excerpt from Made relied on by the Examiner simply does not teach a "secondary set of identifying code operable to identify, within said stream, at least one secondary set of one or more external program calls **associated with said primary set of one or more external program calls**" (emphasis added), where the "primary set of one or more external program calls match[es] one or

more rules indicative of malicious computer program activity from among a set of rules" (emphasis added), in the context claimed by applicant.

Still with respect to independent Claims 1, 18 and 35, the Examiner has again relied on Col. 6, lines 12-24; and Col. 11, lines 46-60 from the Made reference to make a prior art showing of applicant's claimed "modifying code operable to modify said set of rules such that said at least one secondary set of one or more external program calls are more strongly associated with malicious computer program activity" (see this or similar, but not necessarily identical language in the independent claims).

Applicant respectfully points out that the Made reference excerpts relied upon by the Examiner merely teach "extracting a behavior pattern and sequence from a modified, new, unknown or suspect program," and that "[t]he behavior pattern is preferably used to analyze the behavior of the unknown program to determine if the behavior of the unknown program is malicious" (Col. 6, lines 13-17 – emphasis added). Such excerpts from Made also teach that the "ABM engine then analyzes the first executable program and finds that its behavior pattern is altered in a manner indicating that a virus is active" (Col. 11, lines 57-59 – emphasis added).

However, applicant respectfully asserts that analyzing "the behavior pattern of the unknown program," and detecting active viruses based on whether an executable program's behavior pattern is altered, as in Made, clearly fail to teach "modifying code operable to modify said set of rules such that said at least one secondary set of one or more external program calls are more strongly associated with malicious computer program activity," (emphasis added), as claimed by applicant, particularly where the "rules [are] indicative of malicious computer program activity," in the context claimed. Simply nowhere in the Made excerpts relied on by the Examiner is there any teaching or suggestion to "modify said set of rules," as claimed by applicant.

In the Office Action mailed 11/01/2007, the Examiner has referred to Col. 6, lines 25-43 in Made in arguing that "Made discloses modifying the behavior patterns as new

malicious behavior is detected and as more malicious behavior is detected it associated the patterns and the calls that fall within the pattern more closely with the malicious activity."

Applicant respectfully disagrees. Col. 6, lines 25-43 in Made simply teach that "a virtual machine is used to generate a behavior pattern and a sequence," and that "[t]he generated behavior pattern does not change significantly between version updates, but does change dramatically when a virus infects a program." However, simply disclosing that a behavior pattern changes when a virus infects a program, as in Made, does not even suggest that "as more malicious behavior is detected it associated the patterns and the calls that fall within the pattern more closely with the malicious activity" (emphasis added), as the Examiner has noted. Furthermore, a behavior pattern that changes when a virus infects a program, as in Made, does not teach "modifying code operable to modify said set of rules such that said at least one secondary set of one or more external program calls are more strongly associated with malicious computer program activity," (emphasis added), as claimed by applicant, particularly where the "rules [are] indicative of malicious computer program activity," in the context claimed.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the Made reference, as noted above. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.